International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# AN IMPROVED MECHANISM FOR INVESTIGATION, DETECTION, AND CLASSIFICATION OF IOT BOTNET ATTACKS

Vikrant[1*], Dr. Gesu Thakur[2]

[1]Research Scholar, College of Smart Computing, COER University, Roorkee, Uttarakhand, India

[2]Professor, College of Smart Computing, COER University, Roorkee, Uttarakhand, India

## Abstract

Many industries and scientific societies are now interested in Internet of Things (IoT) technology because of its many intelligent uses. In particular, the quantity of suspicious activity such as IoT botnets and extensive cyberattacks, has sharply increased, as has the number of IoT devices that are vulnerable or unprotected. Numerous conventional techniques for detecting botnets struggle to scale up to the demands of secured IoT network. The conventional approach has scalability problems that impact all aspects of the Botnet detection system, including feature extraction, data collecting, storage, and analysis, and are not limited to detection bottlenecks. The main objective of the current study is to create a classification model that can identify different types of IoT botnet attacks. There are several ways to attack the IoT architecture's network and application layers. The proposed approach is to evaluate how safe and, more importantly, resilient commonplace IoT devices can be against the Mirai and Gafgyt botnets. In this article, we have crafted and implemented four different models such as random forest, autoencoder, linear, and threshold classification that is utilized to detect and classify the IoT botnet attacks. The validation has been done by using zero-day attack classification.

**Keywords**: IoT Botnet, IoT Botnet classification, Mirai, Gafgyt, IoT Threat Vectors, IoT Botnet Detection.

### Introduction

A large number of inexpensive IoT devices come brand-new with pre-configured settings. They are susceptible to malware that is now hiding on the Internet because the makers are not adequately protecting them. The rise of IoT botnets presents a significant challenge to cybersecurity. These IoT botnets exploit the vulnerabilities of interconnected IoT devices, leveraging their collective computing power to execute large-scale attacks [1]. The rapid growth of IoT devices increases the potential attack surface. Many IoT devices are deployed with default credentials or insufficient security mechanisms, making them prime targets for botnet recruitment. Devices with limited resources and heterogeneity differ greatly in terms of operating systems, functionality, and design. Standardized security solution creation is made more difficult by this variety. Furthermore, the deployment of strong security measures

Received: July 18, 2025

like encryption and sophisticated intrusion detection systems is limited by the resource constraints of many devices. diverse manufacturers frequently adhere to diverse protocols, which results in inconsistent security procedures and a lack of unified security standards and protocols for IoT networks. Because of this fragmentation, attackers can more easily create botnets by taking advantage of weak points in the ecosystem. IoT botnets are made to function covertly, frequently imitating typical device activity to avoid discovery. Traditional intrusion detection systems have a hard time spotting malicious activity because attackers use strategies like encrypted communications, randomized IP addresses, and low-and-slow traffic generation. IoT botnets of today, such as Mirai and its variations, are getting increasingly complex. They employ sophisticated command-and-control (C2) structures, such as peer-to-peer networks, and take advantage of zero-day vulnerabilities to thwart takedown attempts [2]. The size and strength of the botnet can grow rapidly once a compromised device infects other devices.

As demonstrated by the record-breaking attacks carried out by Mirai, whose source code was made public and made available for any malevolent actor to set up and exploit, this scalability is particularly risky in distributed denial-of-service (DDoS) attacks. A combination of improperly and ineffectively used software assets puts customers at danger of a total compromise (Figure 1). In this investigation, Mirai libraries have been used to configure and target four different IoT devices [3]. According to the experiment results, when the four devices were deployed with their original configuration, three of them became infected because they were vulnerable to the Mirai malware. This illustrates how the default security settings are insufficient to give customers adequate protection levels, leaving their devices exposed. The correct device configuration countermeasures to harden the devices against this botnet were identified by examining the Mirai libraries and their attack routes. These countermeasures were successfully confirmed through experimentation.

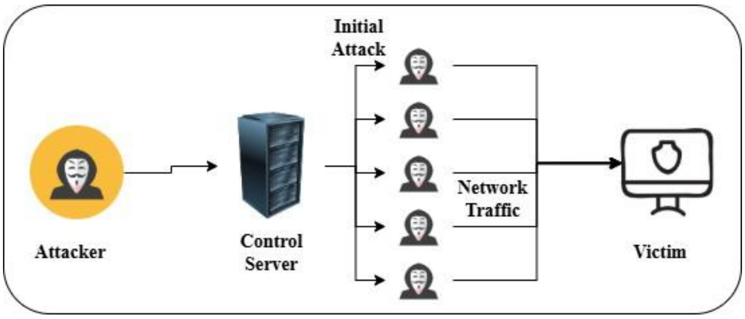

Fig. 1. IoT Botnet Attack Scenario

It's the first time that a comprehensive digital forensic case study on Mirai, one of the most well-known kinds of IoT bot malware, has been accessible. With a record-breaking speed of 1.1 Tbps [4], the Mirai-run botnet network, which is employed in DDoS attacks, comprises over 100,000 IoT devices aimed at households. Although previous studies have thoroughly examined the botnet architecture and the Mirai source code (as well as its variations) using standard static and dynamic malware analysis tools, they have not done so for compromised devices or Mirai network devices. In order to develop a fully functional Mirai botnet network

Received: July 18, 2025

architecture, some researchers thoroughly investigated the Mirai botnet server through forensic analysis. They looked into the network packets that came from the attacker's terminal, database server, CNC server, scan receiver, loader, and other forensic evidence that was left on them. They also describe how a forensic investigator did not need to physically visit the botnet server to retrieve some of these artifacts. In addition to the data that can be gathered (such as the IP addresses of bot participants), the findings of these studies can provide forensic investigators with crucial information regarding which device to target for study and acquisition in order to get valuable data [5] [6]. Protecting an IoT system against Mirai botnet and DDoS attacks, IoT has spread widely across all industrial and application domains, including transportation, healthcare, and the military. A novel hybrid detection and mitigation mechanism is utilized for the detection and analysis of IoT botnet. Furthermore, one of the dangerous attacks, named DDoS, represent a serious threat to the operation of IoT application DDoS attacks at the network layer seriously harm the data transmission channel, resulting in data loss or collapse. Several research focuses on a unique discovery and mitigation of Mirai and DDoS attacks in IoT contexts.

It is necessary to safeguard IoT devices against botnet activity. This study outlines a novel method that makes it possible to identify efforts to compromise IoT devices. For this, a mathematical model of assault on IoT devices is developed using game theory. This method makes it possible to stop attempts to break the IoT. IoT devices are increasingly being used. Although these devices have the potential to enhance many application areas, their lack of security can be used by criminals to create extensive botnets [7]. Among the application domains that this paradigm presently covers are smart cities, smart homes, manufacturing, and agriculture. Commonplace items and sensors are transformed into Internet nodes via IoT, which enables them to communicate with people and other devices to carry out their tasks. The majority of IoT devices, in contrast to conventional PCs and smartphones, are not made with the primary function of providing Internet connectivity. They do, however, collect and transmit a lot of information about the environment in which they work, much of its security-sensitive. They are also capable of receiving remote commands to respond to a range of situations, including potentially fatal ones. Due to their lack of protection compared to other computing devices and their involvement in security-sensitive tasks, they are an ideal target for malicious activities.

Detecting IoT botnets requires a multifaceted approach that combines traditional network security methods with advanced analytics and machine learning techniques. Signature-based detection systems, such as intrusion detection systems (IDS), are widely used to identify known patterns of malicious behavior; however, their effectiveness is limited against novel or obfuscated attacks [8]. To address this, anomaly-based detection methods analyze deviations from normal IoT device behavior, including unusual traffic volumes, unexpected communication patterns, or irregular time intervals. Machine learning models may distinguish between malicious and benign traffic by examining flow characteristics like packet size, connection time, and protocol usage. This is especially true for models trained on network traffic datasets like CICIoT. By using device profiling to identify unusual activity, such as an IoT thermostat abruptly establishing outgoing connections to dubious domains,

Received: July 18, 2025

behavioral analysis also plays a significant part. To find intricate patterns in massive amounts of traffic data, advanced methods include deep learning models such as RNN and CNN. Organizational sharing of threat intelligence improves botnet detection by utilizing shared understanding of new threats and indications of compromise (IOCs) [9]. Researchers can learn about botnet tactics, methods, and procedures (TTPs) by using honeypots, which imitate weak IoT devices and draw in attackers. While blockchain technology can offer a tamper-proof record of device activity, supporting accountability and forensic analysis, distributed monitoring across edge devices and gateways allows real-time detection in decentralized IoT networks. Comprehensive protection is provided by hybrid detection systems that integrate several strategies, such as behavior-, anomaly-, and signature-based methods; nonetheless, issues like false positives and computational overhead still exist. In order to stay ahead of attackers as IoT botnets develop, coordinated and adaptive tactics backed by ongoing learning and updating are essential [10].

In order to protect the Internet of Things from the Mirai Botnet, several researchers also used a special blockchain-based architecture. A method for establishing host connections that divide the network into distinct Autonomous Systems (AS) is suggested. It keeps and disseminates a list of the IP addresses of different hosts connected to an AS via blockchains, highlighting which of them have been deemed harmful. To ascertain whether a host is infected with malware, each AS keeps an eye on network communication activity and compares the total number of packets sent by the host with a predetermined threshold value. The suggested method is developed by determining an appropriate value for the hazardous threshold using a specially built simulator [11]. The findings show that the suggested technique effectively prevents malicious packets from leaving the compromised host, hence preventing any impact on the victim's reaction time. The block propagation delay is also forecasted for different consensus methods and AS sizes, and a scalability study is carried out. The findings showed a 95% accuracy rate in detection. The IoT, which has applications in homes, businesses, and healthcare, is one of the most popular technologies of the past few years. A game-theoretic approach to defend IoT devices against the Mirai Botnet. Mirai is the largest known botnet to compromise the Internet of Things. During its peak activity, the botnet successfully attacked about 100,000 machines. Consequently, at that time, 170,000 of the roughly 1.2 million infected IoT devices were in use [12].

One of the most important tasks in improving cybersecurity and protecting the quickly expanding IoT is classifying IoT botnets. Due to inherent vulnerabilities, IoT devices are becoming more and more common in households, businesses, and critical infrastructure, making them ideal targets for botnet exploitation. The development of focused mitigation techniques is made easier by the ability to identify particular botnet kinds, their activities, and the hazards they pose through effective classification. By identifying malicious behavior early on, it helps lessen the impact of large-scale attacks like DDoS or data exfiltration. By distinguishing between hostile and benign traffic, classification algorithms help prevent false alarms from interfering with the proper operation of IoT devices [13]. Furthermore, developing strong intrusion detection and prevention systems that are adapted to changing threats is made easier by knowing the traits and attack methods of various botnet families,

Received: July 18, 2025

such as Mirai, Gafgyt, or Mozi. Proactive threat modeling and protection are made possible by classification, which also offers insights into the tactics, methods, and procedures (TTPs) used by attackers. It facilitates the sharing of threat intelligence in real time, encouraging cooperation between governments, organizations, and researchers in the fight against international cyberthreats. Additionally, classification models—which are frequently driven by machine learning—continually learn from fresh data, adjusting to new botnet variations and zero-day vulnerabilities. Whether the botnet activity is denial-of-service, spamming, reconnaissance, or credential theft, companies can better deploy resources to address the most critical vulnerabilities by determining the type of botnet activity. Furthermore, forensic investigation benefits from precise botnet classification since it helps identify attack sources, comprehend their effects, and fortify legal and regulatory frameworks [14]. Additionally, by encouraging the creation of robust device architectures and network protocols, it spurs innovation in IoT security. IoT botnet classification is ultimately essential for preserving the integrity of the networked digital ecosystem, guaranteeing the dependability of smart devices, and preserving confidence in IoT technology.

In the current research, classification and detection mechanisms are utilized for IoT botnet. The experimental setup has been done with distinct machine learning algorithms with CICIoT2023 dataset. First, the data exploration is done for the identification of exceptional classifiers, and anomaly values. Then feature extraction is done by using recursive feature elimination and selection of top 10 features based on their relativeness. Four distinct models have been building such as linear, random forest, autoencoder, and threshold classification. The contribution of the paper is as follows:

- To propose a model for the detection and classification of the DoS and DDoS data packet flow from the IoT network packets.
- To extract the top features by using recursive feature elimination.
- To test the model on the dataset and validate the proposed approach with 98% accuracy, 99% recall score.

The remaining paper can be categorized into the following sections: section II focuses on the latest research which has been conducted for the detection and identification of IoT botnet techniques. Section III discussed proposed methodology with the experimental setup configuration. Section IV focused on the dataset description with number of features and selected features of CICIoT 2023 dataset. Section V demonstrated the results with discussion of results. Finally, section VII concludes the article.

## Literature Review

An overview of previous research on Botnet Detection has been conducted and is presented in the current section. IoT Botnet Attack Detection via Networks [15] this paper's Deep Autoencoders approach for identifying IoT botnet attacks uses deep autoencoders for every device, which are trained using statistical features taken from benign traffic data. Anomalies found in newly collected (potentially compromised) IoT device data could be a sign that the device is compromised. Here, the Mirai and Bashlite botnets are in use. After the autoencoder

Received: July 18, 2025

training and optimization phase, three more frequently used anomaly detection algorithms—Local Outlier Factor (LOF), One-Class SVM, and Isolation Forest—were trained using the same (benign) data. Similar to how they adjusted the autoencoders, they also optimized their hyperparameters. Lastly, the C&C servers of BASHLITE and Mirai were used to perform all attacks for the same amount of time. The deep autoencoders demonstrated superiority for the majority of devices in terms of TPR, FPR, and detection time. Deep architectures' capacity to learn nonlinear structure mapping and approximate complex functions is most likely the cause of this. Furthermore, the lower dimensionality in the hidden layers constrains the complexity of deep autoencoders, making it impossible for them to learn the trivial identity function. Consequently, frequent patterns are typically better fitted by deep autoencoders than unusual ones [16].

Enhancing IoT Botnet Research Employing a Network Layer Adaptive the suggested remedy can alter network-layer traffic according to the malware's actions [17]. They investigated the Mirai and Bashlite botnet families, which allowed them to identify attack targets, stop attacks on other systems, and modify commands delivered to infected devices by the botnet controller. In an analysis setting, this study presents an approach for managing network traffic produced by IoT malware. They take advantage of the network layer's flexibility more than they do the network traffic that the sample generates [18]. The strategy seeks to: monitor the communication channel, deploy efficient defenses against attacks, fingerprint the botnet C&C, and alter commands directed at the compromised device. An ensemble data pre-processing step that is applied beforehand is the foundation of the weighted anomaly-based intrusion detection system (IDS) proposed by paper [19].

Although there are many non-smart connected cyber-physical devices that use this technology, a variety of characteristics, such as wireless communications, diversity, scalability, absence of local security measures, and node mobility, have led to serious security issues [20]. Using an ensemble data pre-processing technique and a machine learning anomaly-based intrusion detection system, the authors provided a framework for identifying botnet attacks in Internet of Things networks. The proposed framework, which has a detection accuracy of 99.7% with detection times ranging from 30 to 80 seconds, is analyzed and compared for many learners using a shared dataset.

Investigators [21] Distributed cloud-based architectures have been proposed for deep learning and botnet phishing attacks. At the application layer, the concept's two main security elements cooperate to identify distributed denial of service (DDoS) and phishing. (1) an application layer distributed denial of service (DDoS) and phishing detection model for distributed convolutional neural networks (DCNNs) integrated into Internet of Things (IoT) devices as micro-security add-ons; and (2) a back-end cloud-based temporal Long-Short Term Memory (LSTM) network model for Botnet attacks. One of the main benefits of the [22] proposed method might be the capacity to carry out different levels of detection at the client and back-end server by utilizing the dispersed processing power of client IoT devices and computationally capable servers.

Received: July 18, 2025

In order to differentiate botnets from legitimate activity in the application layer with regard to DNS services, the authors [23] proposed a two-level deep learning-based botnet detection method. The first level of the system computes the similarity metrics of DNS requests based on a preset threshold using Siamese networks to select the most frequently utilized DNS data across Ethernet connections. The second level of the framework proposes a domain generation algorithm (DGA) that uses deep learning architectures to distinguish between common and uncommon domain names. The framework is very scalable on a commodity hardware server due to its DNS data possibilities.

In order to gain understanding of this quickly changing threat, the authors [24] examined passive, macroscopic empirical data. In addition to identifying, revealing, and closely analyzing "in the wild" IoT botnets, the author plans to categorize and deduce compromised Internet-scale IoT by merely observing one-way network traffic. First, the field of Internet measures is greatly advanced with the presentation of a revolutionary darknet-specific sanitization [25]. Then, using only darknet data, the suggested methodology [26] creates a binary classifier based on a CNN and active measurements that may identify compromised IoT devices.

Venkatraman, S., B. Surendiran, and P. Arun Raj Kumar [27] proposed a Nave Bayesian approach that combines conceptual and semantic similarities to stop spam emails. The performance of spam email detection techniques is improved in smart networks by this way. The device can recognize whether the Trojan is masquerading as a genuine mail server. Better zero-day protection, lower administrative expenses, and no backscatter are the results. In order to identify and steer clear of unsolicited emails sent by Internet of Things devices, it uses conceptual and semantic similarity-based spam for content analysis when examining smart settings. It can help with hosted cloud, cloud, and dedicated on-premises. Xia, Hui, and colleagues [28] introduced a dynamic model of botnet propagation, such as the IoTBSI model, to examine how two social variables, such as device spread capability and device identification ability, affect botnet formation. evaluates how different information transmission routes' varying degrees of trustworthiness and nonMarkovian social contagion power affect intelligent systems' ability to discriminate. Social theory divides the capacity for identification into two groups: irrational and rational identification.

Using communication graph models to identify botnet trends was the main goal of A Novel Botnet Detection using Communication Graphs (2023). The main method used statistical analysis in conjunction with graph-based anomaly identification. It finds anomalous communication patterns, increasing the detection rates. As graph algorithms are being improved to function in real-time for extensive IoT deployments. This study's systematic review of IoT botnet DDoS attacks (2024) examined related detection methods and examined DDoS attacks in IoT networks [29]. The classification of machine learning methods for identifying IOT botnets was their primary focus. To improve detection, the authors outlined the vulnerabilities and suggested an integrated architecture. To respond to changing threats, the future scope considers the new AI models. To detect IoT botnets, the current study compares machine learning and deep learning algorithms. To identify IoT botnets, they have

Received: July 18, 2025

assessed various performance metrics using various machine learning and deep learning methods. For thorough detection, a hybrid model may be used in the future. Blockchain's potential to improve botnet detection systems was examined by the writers. Distributed ledger integration was used to track C&C communications. False positives are decreased and data integrity is enhanced. Future research will focus on using blockchain analytics to create secure and self-sufficient IoT ecosystems. In this study, a model for identifying and assessing the Mirai botnet is proposed [30]. The impact and intricate architecture of the Mirai botnet with propagation model were also covered. Enhancing the designated attack vectors is the main goal of the result. There may be zero-day vulnerabilities linked to changing botnet architectures in the future. To identify and detect IoT botnets, researchers used an autoencoder-based approach. Enhancing IoT traffic and optimizing autoencoders can increase the performance of IoT devices [31]. Some of the research gaps for identifying and recognizing IoT botnets have been found based on the thorough literature study. The current research is to classify the distinct IoT botnet attacks by using intelligent algorithms such as linear classification, threshold classification, random forest classification, and autoencoder classification. The model is built on CICIoT 23 dataset with reduced number of features.

## Proposed Methodology

In this section, we discuss the proposed scenario of the experimental setup and configuration details.

### 3.1 Experimental Setup Configuration

The CICIoT23 dataset's experimental configuration was painstakingly created to produce thorough traffic data across a variety of IoT devices and assault scenarios. This dataset includes network traffic from 105 IoT devices that were targeted by 33 different kinds of assaults. These attacks were divided into seven main attack classes: web-based, Mirai botnet, brute-force, reconnaissance, spoofing, DDoS, and DoS. To guarantee the dataset's dependability and suitability for research, the trials were conducted in a controlled setting. Several IoT devices, including cameras, smart thermostats, and home assistants, were part of the IoT network environment and were connected to a local area network (LAN). To ensure variation in the collected data, the traffic generating tools were utilized to mimic criminal activity and real-world device communication. A variety of vectors and payloads were covered by the methodical deployment of each attack type. For example, reconnaissance attacks imitated hostile network scanning activities, whereas DDoS assaults used high-volume packet flooding techniques. In order to differentiate between benign and malicious activity, the trials also included benign traffic [32].

High-performance servers with Intel Xeon processors, at least 64 GB of RAM, and high-speed solid-state drives (SSDs) to effectively handle massive amounts of data were part of the system configuration for data collecting and processing. Tools such as Wireshark and tcpdump were used to record network traffic, guaranteeing detailed data collection at the packet level. To handle the vast amount of data produced over weeks of nonstop observation, sophisticated storage techniques were used. Specialized tools were also incorporated to label and preprocess the data, such as feature extraction tools for examining traffic attributes

Received: July 18, 2025

including protocol usage, packet inter-arrival periods, and flow duration. The configuration incorporated intrusion detection and prevention systems (IDPS) to cross-verify abnormalities in order to improve data integrity. Additionally, Docker containers and virtual machines (VMs) were used in the experimental environment to isolate attack simulations and avoid accidentally contaminating benign traffic [33]. In order to clean and standardize traffic data and guarantee compatibility with machine learning models, data preprocessing required the use of Python packages such as pandas and scikit-learn. The suggested experimental work methodology is depicted in Figure 2.

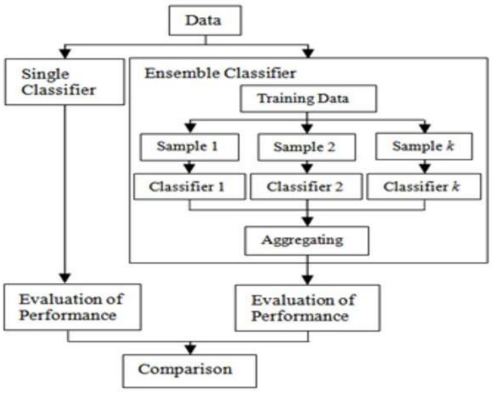

Fig. 2. Proposed Methodology

3.2 Machine Learning Algorithms

To differentiate malicious traffic from legitimate IoT device communications, a comprehensive and adaptable framework is provided by the suggested methodology for classifying IoT botnet traffic, which integrates distinct machine learning algorithms, including linear classification, threshold-based classification, Random Forest classification, and autoencoder-based classification. Each classifier contributes according to its strengths in an ensemble system using the integrated technique. The linear models can quickly identify known attack types through threshold classification and filtering. More intricate patterns are handled by Random Forest and autoencoders [34]. Using specific performance criteria including accuracy, precision, recall, and F1-score on the CICIoT23 dataset, the suggested model is verified. The improvement includes autoencoder retraining to adjust to new threats and dynamic threshold updating. Robust detection capabilities, interpretability, and computational efficiency are all balanced by this hybrid methodology.

*Linear Classification:* As a baseline method for classifying IoT botnet traffic, linear classifiers like logistic regression or SVM are used. The underlying premise of these models is that malicious and benign communications are separated by a linear decision boundary [35]. To increase classification accuracy, pertinent data including protocol usage, packet size, and flow time are retrieved and standardized. The likelihood of malicious activity is predicted by a logistic regression model, and a predetermined threshold (e.g., 0.5) is used to make the choice. While linear classification is helpful when resources are scarce, it is unsuccessful when dealing with complicated datasets that exhibit non-linear patterns, which are prevalent

Received: July 18, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in IoT botnet scenarios. A linear classifier predicts the y class based on different linear inputs x with bias b and weight w such as (equation 1):

$$y = w^T x + b \qquad (1)$$

The classification results are depended on the decision rule in terms of equation 2 such as:

$$\hat{y} = \begin{cases} 1 & if\ w^T x + b \geq 0 \\ 0 & Otherwise \end{cases} \qquad (2)$$

*Threshold-Based Classification:* This approach involves setting predefined thresholds for specific network features to classify traffic as benign or malicious. Features such as unusually high packet rates or prolonged connection durations are monitored, and traffic exceeding these thresholds is flagged [36]. It is particularly effective for detecting DDoS or brute-force attacks, which often exhibit extreme values in specific features. Although, it has high interpretability and low computational overhead make it ideal for real-time applications. However, the limited flexibility as it relies heavily on expert-defined thresholds, which may not generalize well to new attack types. The threshold classification is based on the mathematical formula for multifeatured classification described in equation 3:

$$\hat{y} = \begin{cases} 1 & if\ f(x_1, x_2, x_3 \dots \dots, x_n) \geq T \\ 0 & Otherwise \end{cases} \qquad (3)$$

Where $\hat{y}$ represents the predicted value, $f(x_1,\ x_2,\ x_3\ \dots\ \dots\ ,\ x_n)$ is a function that aggregating the multiple features of the dataset and T is the threshold value evaluated based on the prior analysis. In case of IoT botnet detection, the threshold value is depended on the feature value such as (Equation 4):

$$x_{size} \geq\ T_{size} \qquad (4)$$

*Random Forest Classification:* An ensemble learning technique called Random Forest is used to identify intricate non-linear relationships in the data. The model is trained using variables like source IP, port numbers, and payload size on labeled datasets like CICIoT23. A majority vote is produced by the ensemble of decision trees to categorize traffic as either harmful or benign. It works well with a variety of IoT traffic patterns since it is resistant to overfitting and able to handle high-dimensional data. It offers excellent detection accuracy for complex botnets that employ a variety of attack methods, such as Mirai. In comparison to linear models, it uses more computational complexity. The random forest classification can be evaluated based on the equation 5 such as:

$$\hat{y}_{final} = Mode\{T_1(x), T_2(x), \dots \dots ., T_N(x)\} \qquad (5)$$

The classifier aggregates the distinct predictions of the decision tree as $T_1$, $T_2$,….., $T_N$ and able to predict the final classification.

*Autoencoder-Based Classification:* Autoencoders, a type of neural network, are utilized for anomaly detection by reconstructing input data and measuring reconstruction errors. The autoencoder is trained on benign IoT traffic to learn normal patterns. Malicious traffic, which deviates from these patterns, yields high reconstruction errors and is classified as anomalous.

Received: July 18, 2025

It is effective in detecting zero-day attacks and generalizing to unseen attack types. It significantly reduces false positives while identifying subtle deviations in traffic patterns. However, it requires extensive computational resources and training time. The reconstruction error e for a random sample can be evaluated in terms of the equation 6.

$$e = ||x - \hat{x}||^2 \qquad (6)$$

On the basis of the reconstruction error and threshold values, the class of the sample decides weather it belongs to malicious or benign traffic (Equation 7).

$$\hat{y} = \{\begin{matrix} Malicious & if\ e \leq T \\ Benign & if\ e > T \end{matrix} \qquad (7)$$

### Dataset Description

A comprehensive and state-of-the-art dataset, the CICIoT 2023 dataset was created to support IoT security research and development. Because the dataset was painstakingly curated by conducting a range of cyberattacks on various IoT devices, it is a priceless tool for researching criminal activity, creating detection systems, and enhancing IoT security frameworks. 105 IoT devices' network traffic data is included in the CICIoT 2023 dataset, which records both benign and malevolent activity. Thirty-three cyberattacks are simulated in the dataset, which is divided into seven main attack types: DDoS, DoS, Web-based, brute-force, spoofing, and Mirai Botnet attacks. Because of the variety of devices and attack methods, CICIoT 2023 is one of the most extensive datasets available for IoT security research. The IoT network was used to build the CICIoT23 dataset because fraudsters are becoming more and more targeted. Internet of Things devices are commonplace and have built-in flaws include poor authentication, no encryption, and little processing power. Safeguarding IoT devices from cyber threats becomes crucial as they become more integrated into vital infrastructure. To close this gap, CICIoT 2023 gives academics access to real-world traffic data for both malicious and benign scenarios.

Both harmful and normal network traffic data were gathered for the CICIoT 2023 dataset. typical traffic information obtained from Internet of Things devices working normally, free from outside threats or interference. The valid device-to-device and device-to-server communications are reflected in this traffic. the harmful traffic data produced by simulating the 33 different kinds of cyberattacks on the 105 devices. The CSV files in the dataset are used to extract network traffic flow-based characteristics. These attributes, which represent different aspects of network communication, are extracted from packet captures (PCAP files). The collection comprises information from a wide variety of Internet of Things devices, such as wearable technology, cameras, smart thermostats, door locks, smart speakers, and industrial IoT equipment. From residential networks to industrial systems, the dataset's diversity guarantees that it accurately depicts real-world IoT contexts.

Table I. CICIoT 2023 Dataset Features

| Feature | Unique | Feature Name | Remark |
|---|---|---|---|

Received: July 18, 2025

| Rank | Values | | |
|---|---|---|---|
| 1 | 5L | Flow Duration | Shows the network duration in microsec. |
| 2 | 10 | Total Bwd Packets | Number of packets shared backward. |
| 3 | 10 | Total Fwd Packets | Number of packets shared forward. |
| 4 | 2L | Total Length of Bwd Packets | Packet size sent backward |
| 5 | 1.5L | Total Length of Fwd Packets | Packet size sent forward |
| 6 | 5K | Mean length Fwd Packet | Length of packets sent in forward direction. |
| 7 | 10K | Flow IAT Mean | Packets within a flow with Mean time inter-arrival. |
| 8 | 1K | Flow IAT Min | Packets in a flow with minimum time inter-arrival. |
| 9 | 100 | Active Duration | Time during which the flow was active. |
| 10 | 1K | Idle Duration | Time during which the flow was idle. |

The CICIoT 2023 dataset is a groundbreaking contribution to IoT security research, offering a realistic and diverse set of network traffic data. By addressing a wide range of attack types across numerous devices, it empowers researchers to develop advanced security mechanisms tailored to the IoT ecosystem. Whether used for IDS development, machine learning experiments, or traffic analysis, the dataset serves as a cornerstone for advancing the state of IoT security. Some attack types may be underrepresented, which could bias machine learning models. The rich feature set can be computationally expensive to process, necessitating feature selection or dimensionality reduction techniques.

## Results and Discussion

Received: July 18, 2025

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This section shows the distinct results and classification of the distinct machine learning models. Figure 3 categorizes the IoT-based cyberattacks into different types, with their corresponding frequencies. The most frequent attack type is DDoS-LOIC-UDP, with over 30,000 occurrences, followed by various other DDoS attacks like DDoS-UDP and DDoS-SYN Flood. Reconnaissance attacks and other classes, such as brute force and Mirai botnet-related attacks, show progressively fewer samples. This distribution highlights the dominance of DDoS attacks in the dataset and the variability in attack types, emphasizing the dataset's utility in developing robust intrusion detection and classification systems.

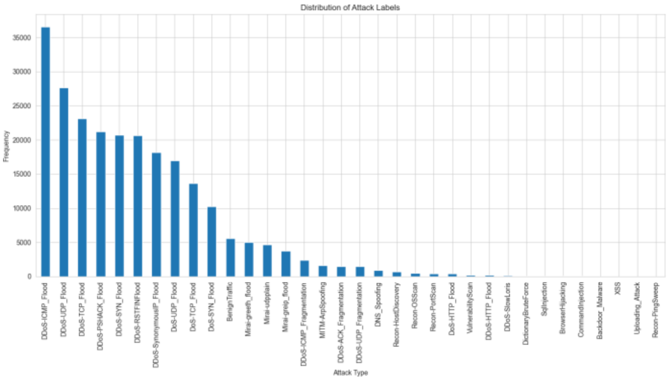

Fig. 3. Distribution of Attack Labels

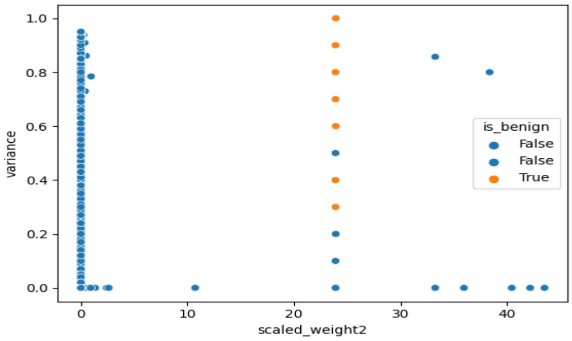

Fig. 4. Scaled Weights vs Variance

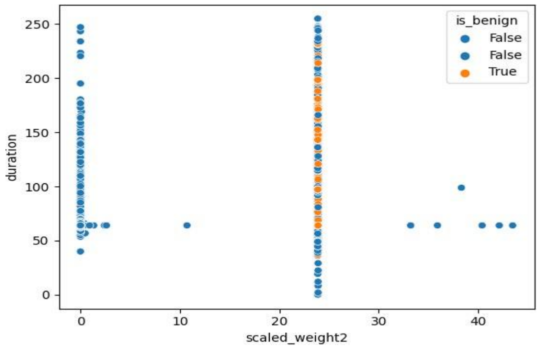

Fig. 5. Scaled Weights vs Duration

Figure 4 shows the scatter plot that illustrates the relationship between the feature scaled_weight2 and variance, with data points classified as benign (orange, "True") or malicious (blue, "False"). Most benign data points cluster around specific values of

Received: July 18, 2025

scaled_weight2, while malicious points are more distributed. This plot visually distinguishes attack patterns from benign traffic. Figure 5 shows the relationship between scaled_weight2 and duration, with data points labeled as either benign or malicious. Benign points are clustered at specific values of scaled_weight2, around 20, while malicious points are more widely distributed. This distinction highlights potential differences in traffic behavior.

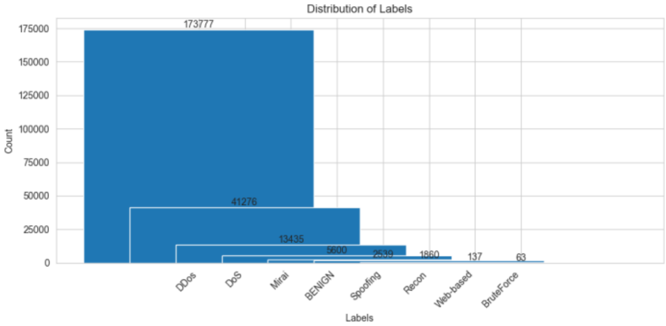

Fig. 6. Distribution of Labels

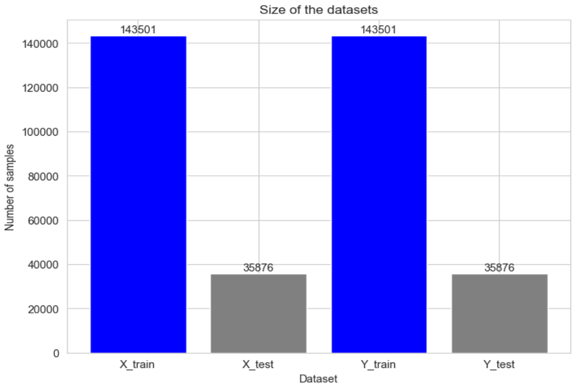

Fig. 7. Dataset classification for training and testing

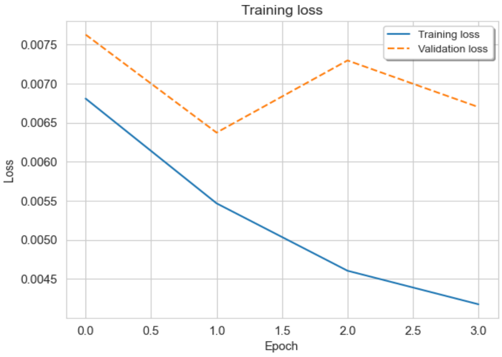

Fig. 8. Training and Validation Losses

Figure 6 shows the bar chart that provides the distribution of labels in the dataset. Most traffic in the dataset is associated with DDoS (173,777 instances), followed by DoS (41,276) and Mirai (13,435). Benign traffic comprises a smaller portion (5,000), with even fewer instances of Spoofing, Reconnaissance, Web-based, and Brute Force. Figure 7 shows the dataset classification for training and testing purposes. The sample data is segregated in X_train, X_test, y_train, and y_test for training and testing. The figure 8 shows the training and

Received: July 18, 2025

validation loss over 3 epochs. Training loss decreases from 0.0075 to approximately 0.0045, indicating consistent improvement. Validation loss starts around 0.0075, fluctuates slightly, and ends near 0.0065. The higher validation loss compared to training loss suggests slight overfitting, with noticeable stability by epoch 3.

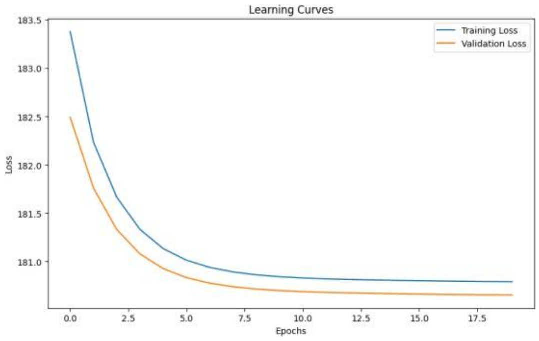

Fig. 9. Quantized Autoencoder Classification

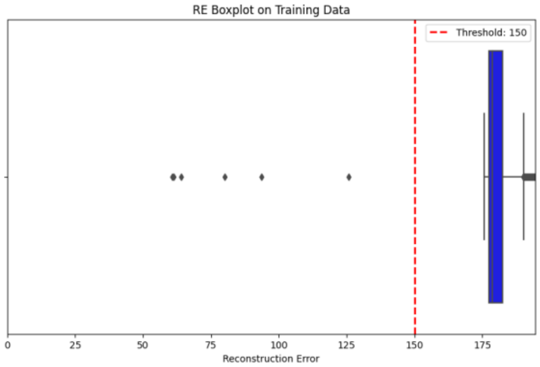

Fig. 10. Reconstruction error Boxplot on training data

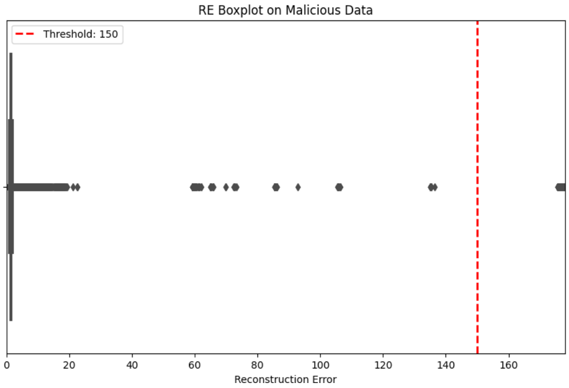

Fig. 11. Reconstruction error Boxplot on Malicious data

The figure 9 shows the learning curves for a quantized autoencoder model's training and validation loss across epochs. Both losses decrease, indicating the model is learning effectively. The gap between curves is small, suggesting minimal overfitting. Training loss stabilizes slightly below validation loss, demonstrating consistent generalization without severe overtraining. The figure 10 is a boxplot showing reconstruction errors (RE) on training

Received: July 18, 2025

data. The figure shows the maximum errors below 150, with the threshold marked as 150 (red dashed line). A few outliers range from 75 to 125. The majority of data points cluster around 175, suggesting most errors are within this range. The figure 11 is a boxplot of RE for malicious data, showing a threshold at 150 (dashed red line). Majority of errors are clustered between 0 and 20, with several outliers reaching up to approximately 160. Most data points fall well below the threshold, indicating low reconstruction errors for the majority. While the figure 12 shows a boxplot of reconstruction errors for validation of the benign data, with a threshold at 150. Most errors range between 160 and 175, exceeding the threshold. A few outliers are below the threshold, around 125. This indicates higher reconstruction errors for benign data compared to the threshold. Table I shows the distinct performance parameters such as accuracy, precision, recall, F1-score, and confusion matrix for 4 machine learning classifiers. The linear classification performed well with 98.6% accuracy and good number of true positives.

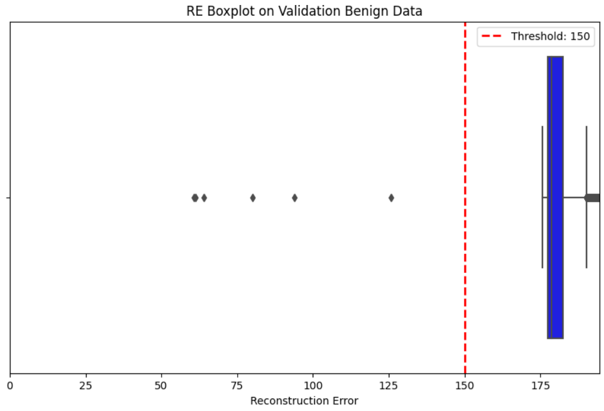

Fig. 12. Reconstruction error Boxplot on Benign data

Table I. Performance parameters with 4 distinct classification models

| Model | Precision | Accuracy | F1 Score | Recall | Confusion Matrix |
|---|---|---|---|---|---|
| Linear Classification | 0.69640 | 0.98695 | 0.73999 | 0.78942 | [[904216, 7557], [4624, 17334]] |
| Threshold Classification | 0.56579 | 0.98195 | 0.72262 | 0.99973 | [[894926, 16847], [6, 21952]] |
| Autoencoder Classification | 0.5655 | 0.981951 | 0.7221 | 0.9997 | [[894925, 16848], [6, 21952]] |
| Random Forest Classification | 0.57553 | 0.97957 | 0.53485 | 0.49954 | [[903683, 8090], [10989, 10969]] |

Received: July 18, 2025

## Conclusion

The current research highlights the critical importance of addressing IoT botnets, which pose significant threats to network security by exploiting vulnerable IoT devices for large-scale cyberattacks. By analyzing IoT botnet dataset such as CICIoT 2023, which includes various attack types (e.g., DDoS, DoS, and Mirai), can better understand attack patterns and behavior. Distinct machine learning classification methods such as linear classification, threshold-based classification, random forests, and autoencoders, robust models are implemented for detecting and classifying IoT botnet traffic. The proposed methodology illustrates promising outcomes in terms of accuracy, confusion matrix, and threshold level 150 for classification of malicious and benign IoT network traffic. The use of feature selection and advanced classification techniques not only improves detection rates but also contributes to building robust systems capable of real-time implementation in resource-constrained IoT environments. In future work, the real-time detection of the IoT network, adoptive solution, and resilient IoT network.

## References

[1] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, “Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication,” IEEE Access, vol. 8, pp. 60539–60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[2] Y. Xing, H. Shu, H. Zhao, D. Li, and L. Guo, “Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation,” Mathematical Problems in Engineering, vol. 2021. Hindawi Limited, pp. 1–24, Apr. 14, 2021. doi: 10.1155/2021/6640499.

[3] S. Verma et al., “DNNBoT: Deep Neural Network-Based Botnet Detection and Classification,” Computers, Materials &amp; Continua, vol. 71, no. 1. Computers, Materials and Continua (Tech Science Press), pp. 1729–1750, 2022. doi: 10.32604/cmc.2022.020938.

[4] K. Sahlmann, V. Clemens, M. Nowak, and B. Schnor, “Mup: Simplifying secure over-the-air update with mqtt for constrained iot devices,” Sensors (Switzerland), vol. 21, no. 1, pp. 1–21, Jan. 2021, doi: 10.3390/s21010010.

[5] M. Panda, A. A. A. Mousa, and A. E. Hassanien, “Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks,” IEEE Access, vol. 9, pp. 91038–91052, 2021, doi: 10.1109/ACCESS.2021.3092054.

[6] S. Hosseini, A. E. Nezhad, and H. Seilani, “Botnet detection using negative selection algorithm, convolution neural network and classification methods,” Evolving Systems, vol. 13, no. 1, pp. 101–115, Feb. 2022, doi: 10.1007/s12530-020-09362-1.

[7] S. Bagui and K. Li, “Resampling imbalanced data for network intrusion detection datasets,” J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-020-00390-x.

[8] M. Catillo, A. Pecchia, and U. Villano, “A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection †,” Applied Sciences (Switzerland), vol. 13, no. 2, Jan. 2023, doi: 10.3390/app13020837.

Received: July 18, 2025

[9] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, “Botnet Attack Detection in IoT Using Machine Learning,” Comput Intell Neurosci, vol. 2022, 2022, doi: 10.1155/2022/4515642.

[10] T. N. Nguyen, Q. D. Ngo, H. T. Nguyen, and G. L. Nguyen, “An Advanced Computing Approach for IoT-Botnet Detection in Industrial Internet of Things,” IEEE Trans Industr Inform, vol. 18, no. 11, pp. 8298–8306, Nov. 2022, doi: 10.1109/TII.2022.3152814.

[11] S. Maurya, S. Kumar, U. Garg, and M. Kumar, “An Efficient Framework for Detection and Classification of IoT Botnet Traffic,” ECS Sensors Plus, vol. 1, no. 2. The Electrochemical Society, p. 026401, Jun. 01, 2022. doi: 10.1149/2754-2726/ac7abc.

[12] T. Hasan et al., “Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach,” IEEE Trans Netw Sci Eng, vol. 10, no. 5, pp. 2952–2963, Sep. 2023, doi: 10.1109/TNSE.2022.3168533.

[13] U. Garg, S. Kumar, and M. Kumar, “INFRDET: IoT network flow regulariser-based detection and classification of IoT botnet,” International Journal of Grid and Utility Computing, vol. 14, no. 6. Inderscience Publishers, pp. 606–616, 2023. doi: 10.1504/ijguc.2023.135344.

[14] S. Thota and D. Menaka, “Botnet detection in the internet-of-things networks using convolutional neural network with pelican optimization algorithm,” Automatika, vol. 65, no. 1, pp. 250–260, Jan. 2024, doi: 10.1080/00051144.2023.2288486.

[15] J. Azimjonov and T. Kim, “Designing accurate lightweight intrusion detection systems for IoT networks using fine-tuned linear SVM and feature selectors,” Comput Secur, vol. 137, Feb. 2024, doi: 10.1016/j.cose.2023.103598.

[16] R. H. Randhawa, N. Aslam, M. Alauthman, M. Khalid, and H. Rafiq, “Deep reinforcement learning based Evasion Generative Adversarial Network for botnet detection,” Future Generation Computer Systems, vol. 150, pp. 294–302, Jan. 2024, doi: 10.1016/j.future.2023.09.011.

[17] S. Mahadik, P. M. Pawar, and R. Muthalagu, “Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT),” Journal of Network and Systems Management, vol. 31, no. 1, Mar. 2023, doi: 10.1007/s10922-022-09697-x.

[18] R. Sharma, S. Mohi ud din, N. Sharma, and A. Kumar, “Enhancing IoT Botnet Detection through Machine Learning-based Feature Selection and Ensemble Models,” ICST Transactions on Scalable Information Systems, Sep. 2023, doi: 10.4108/eetsis.3971.

[19] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” IEEE Communications Surveys and Tutorials, vol. 22, no. 3, pp. 1646–1685, Jul. 2020, doi: 10.1109/COMST.2020.2988293.

[20] E. Gelenbe and M. Nakip, “Traffic Based Sequential Learning During Botnet Attacks to Identify Compromised IoT Devices,” IEEE Access, vol. 10, pp. 126536–126549, 2022, doi: 10.1109/ACCESS.2022.3226700.

[21] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, “A Visualized Botnet Detection System Based Deep Learning for the Internet of Things

Received: July 18, 2025

Networks of Smart Cities," IEEE Trans Ind Appl, vol. 56, no. 4, pp. 4436–4456, Jul. 2020, doi: 10.1109/TIA.2020.2971952.

[22] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection &amp; mitigation in SDN-IoT network," e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 8. Elsevier BV, p. 100543, Jun. 2024. doi: 10.1016/j.prime.2024.100543.

[23] U. Garg, S. Kumar, and A. Mahanti, "IMTIBOT: An Intelligent Mitigation Technique for IoT Botnets," Future Internet, vol. 16, no. 6. MDPI AG, p. 212, Jun. 17, 2024. doi: 10.3390/fi16060212.

[24] B. Bojarajulu and S. Tanwar, "Customized convolutional neural network model for IoT botnet attack detection," Signal, Image and Video Processing, vol. 18, no. 6–7. Springer Science and Business Media LLC, pp. 5477–5489, Jun. 17, 2024. doi: 10.1007/s11760-024-03248-4.

[25] K. Kaur, A. Kaur, Y. Gulzar, and V. Gandhi, "Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies," Frontiers in Computer Science, vol. 6. Frontiers Media SA, Jun. 26, 2024. doi: 10.3389/fcomp.2024.1420680.

[26] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques," Sensors, vol. 24, no. 11. MDPI AG, p. 3571, Jun. 01, 2024. doi: 10.3390/s24113571.

[27] S. Yu, G. Wang, X. Liu, and J. Niu, "Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking Perspective," IEEE Communications Magazine, vol. 56, no. 9. Institute of Electrical and Electronics Engineers (IEEE), pp. 14–18, Sep. 2018. doi: 10.1109/mcom.2018.1701204.

[28] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," Future Generation Computer Systems, vol. 100. Elsevier BV, pp. 779–796, Nov. 2019. doi: 10.1016/j.future.2019.05.041.

[29] S. Lee, A. Abdullah, N. Z. Jhanjhi, and S. H. Kok, "Honeypot Coupled Machine Learning Model for Botnet Detection and Classification in IoT Smart Factory – An Investigation," MATEC Web of Conferences, vol. 335. EDP Sciences, p. 04003, 2021. doi: 10.1051/matecconf/202133504003.

[30] N. A. Hikal and M. M. Elgayar, "Enhancing IoT Botnets Attack Detection Using Machine Learning-IDS and Ensemble Data Preprocessing Technique," Lecture Notes in Networks and Systems. Springer Singapore, pp. 89–102, 2020. doi: 10.1007/978-981-15-3075-3_6.

[31] H. Xia, L. Li, X. Cheng, X. Cheng, and T. Qiu, "Modeling and Analysis Botnet Propagation in Social Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 8. Institute of Electrical and Electronics Engineers (IEEE), pp. 7470–7481, Aug. 2020. doi: 10.1109/jiot.2020.2984662.

[32] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, "A novel graph-based approach for IoT botnet detection," International Journal of Information Security, vol. 19, no. 5. Springer Science and Business Media LLC, pp. 567–577, Oct. 23, 2019. doi: 10.1007/s10207-019-00475-6.

Received: July 18, 2025

[33] I. Ali et al., “Systematic Literature Review on IoT-Based Botnet Attack,” IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers (IEEE), pp. 212220–212232, 2020. doi: 10.1109/access.2020.3039985.

[34] B. Bala and S. Behal, “AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges,” Computer Science Review, vol. 52. Elsevier BV, p. 100631, May 2024. doi: 10.1016/j.cosrev.2024.100631.

[35] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, “The evolution of Mirai botnet scans over a six-year period,” Journal of Information Security and Applications, vol. 79. Elsevier BV, p. 103629, Dec. 2023. doi: 10.1016/j.jisa.2023.103629.

[36] R. Mahajan and M. Kumar, “Autoencoder-Based Botnet Detection for Enhanced IoT Security,” Communications in Computer and Information Science. Springer Nature Switzerland, pp. 162–175, 2023. doi: 10.1007/978-3-031-47055-4_14.

Received: July 18, 2025